UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

NEVILLE MCFARLANE, DEANNA COTTRELL, EDWARD HELLYER, CARRIE MASON-DRAFFEN, HASEEB RAJA, RONNIE GILL, JOHN FRONTERA, SHARIQ MEHFOOZ, and STEVEN PANICCIA, individually and on behalf of all others similarly situated, Plaintiffs, v. ALTICE USA, INC., a New York Corporation, Defendant.	Lead Case No. 20-CV-1297 (consolidated with 20-CV-1410) **AMENDED CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Neville McFarlane, DeAnna Cottrell, Edward Hellyer, Carrie Mason-Draffen, Haseeb Raja, Ronnie Gill, John Frontera, Shariq Mehfooz, and Steven Paniccia (collectively, "Plaintiffs"), individually and on behalf of all other similarly situated individuals (the "Class Members," as defined below), by and through the undersigned Interim Lead Class Counsel William B. Federman of Federman & Sherwood, file this Amended Consolidated Class Action Complaint against Altice USA, Inc. ("Altice" or "Defendant") and allege the following based on personal knowledge of facts pertaining to themselves and on information and belief based on the investigation of counsel as to all other matters.

I. NATURE OF THE ACTION

1. Altice is one of the largest cable TV and communications providers in the United States. It is publicly traded on the New York Stock Exchange under the ticker symbol "ATUS."

Altice's broadband, pay television, mobile, internet, proprietary content and advertising services are used by nearly 5 million subscribers across 21 states through its Altice, Optimum, Suddenlink, and other brands.[1]

2. Between 2015 and 2017, Altice acquired numerous existing businesses in the cable and telecommunications industry, including Suddenlink Communications ("Suddenlink") and Cablevision Systems Corporation ("Cablevision").[2] As part of the acquisitions, Altice acquired the companies' contracts and obligations, existing employees, and records for the companies' former employees.[3]

3. Plaintiffs and the Class Members (as further defined below) are current and former employees, many of whom are also cable subscribers, of Altice who entrusted Altice with their personally identifiable information ("PII"). Defendant betrayed Plaintiffs' trust and that of the other Class Members by failing to properly safeguard and protect their PII and thereby enabling cyber criminals to steal their PII.

4. This class action seeks to redress Altice's unlawful, willful and wanton failure to protect the PII of over 50,000 individuals that was disclosed in a major data breach in November 2019 (the "Data Breach" or "Breach"), in violation of common law and statutory obligations.

---

[1] "Investor Relations," ALTICEUSA.COM, https://investors.alticeusa.com/investors/overview/default.aspx.

[2] With its purchase of Cablevision in 2016, Altice acquired Cablevision's subsidiaries, including Newsday. After owning it for under two years, however, Altice sold Newsday back to Cablevision's prior owners in 2018. *See* Claude Solnik, *Patrick Dolan Becomes Newsday Sole Owner*, LONG ISLAND BUSINESS NEWS (Aug. 1, 2018), https://libn.com/2018/08/01/patrick-dolan-becomes-newsday-sole-owner/. Altice only owned Newsday in full for approximately two weeks, before selling the majority share of Newsday (75%) back to its former owners. After that point, the Newsday human resources department, and not Altice, should have been the entity maintaining and storing Newsday employee PII.

[3] For purposes of this Action, all companies that were owned or acquired by Altice prior to November 2019 are collectively referred to as "Altice" unless otherwise specified.

5. The Data Breach occurred as a result of a phishing campaign that compromised Altice's corporate email accounts. An undisclosed number of Altice's employees, untrained and ill-equipped to protect their accounts from such attacks, provided their login information to cyber criminals. Once provided access to the online credentials, the cyber criminals were able to remotely login to Altice corporate accounts, where they found a treasure trove of Plaintiffs' and Class Members' PII.

6. In one of the Altice accounts there was an unencrypted report (the "Unencrypted Report") that contained the PII of people who ever worked for Altice as well as people who worked for any Altice-owned company. Altice has admitted that the Data Breach gave hackers access to the PII of all of its over 12,000 current employees and gave hackers access to the PII of many former employees as well. In total, 52,846 individuals' PII was compromised in the Breach.

7. The PII on the Unencrypted Report included employees' names, employment information, dates of birth, Social Security numbers, and some drivers' license numbers.

8. Many of the current and former employees, including Plaintiffs McFarlane, Hellyer, Mason-Draffen, Raja, Gill, Frontera, Mehfooz, and Paniccia, were also subscribers to Altice cable television service, and their PII was stolen as part of the same Breach.

9. Due to Defendant's negligence and statutory violations, cyber criminals obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

10. Plaintiffs, including McFarlane, Mehfooz, and Paniccia have already suffered identity theft as a result of the Data Breach, including having unauthorized credit cards being opened in their names. This has and will cause these Plaintiffs significant actual damages and a significant amount of lost time and opportunity.

11. For the rest of their lives, Plaintiffs and the Class Members will have to deal with the danger of identity thieves possessing their PII. Even those Class Members who have yet to experience identity theft have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiffs and Class Members have incurred, and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of PII, loss of privacy, and/or additional damages as described below.

12. Plaintiffs bring this action individually and on behalf of the Class, seeking actual damages, statutory damages, punitive damages, restitution, and injunctive and declaratory relief, along with the reasonable attorney fees, costs, and expenses incurred in bringing this action.

II. THE PARTIES

Plaintiff Neville McFarlane

13. Plaintiff Neville McFarlane is domiciled in and a citizen of Bronx County, New York.

14. McFarlane was an employee of Altice from 1999 to 2017.

15. As part of his employment, McFarlane was required to provide Altice with his PII, including the information compromised in the Data Breach. McFarlane was, and is, also a subscriber of Altice's cable TV service. To subscribe, he was required to provide Altice with his PII, including some of the information compromised in the Data Breach.

16. On January 12 and 13, 2020, McFarlane discovered that a credit card was fraudulently opened using his name, Social Security Number, and other PII. McFarlane's PII was also misused in March 2020, when an identity thief attempted to change his home address.

17. In February 2020, Altice received a breach notification letter from Altice informing him that, as a former employee, his personal information, including name, employment information, Social Security Number, and date of birth were stolen in the November 2019 Breach—just *two months* before the identity theft began. Altice informed McFarlane that some breach victim's driver's license numbers were also compromised, but Altice failed to inform McFarlane whether his driver's license number was among those affected. McFarlane received a letter substantially similar in all material respects to the letters attached hereto as Exhibits 1-3.

18. McFarlane has spent numerous hours responding to the Data Breach and the identity theft that has occurred because of it. Among other things, McFarlane has spent time: (1) corresponding with financial institutions regarding the credit card that was fraudulently opened in his name; (2) monitoring his accounts and personal information; and (3) placing a freeze on his credit report. As a direct and proximate result of the Data Breach, McFarlane will need to purchase a lifetime subscription to identity theft protection and credit monitoring—services which McFarlane has devoted time to exploring in response to the Data Breach.

19. McFarlane has been careful to protect and monitor his identity, and he has never before been a victim of identity theft.

20. To his knowledge, McFarlane has not been the victim of any other data breach.

Plaintiff DeAnna Cottrell

21. Plaintiff DeAnna Cottrell is domiciled in and a citizen of St. Charles County, Missouri.

22. Cottrell was an employee of Suddenlink Communications/Altice from approximately July 2006 to January 2017.

23. As part of her employment, Cottrell was required to provide Suddenlink with her PII, including the information compromised in the Data Breach. When Altice acquired Suddenlink, it acquired her information as well.

24. On February 11, 2020, Cottrell received a breach notification letter from Altice informing her that, as a former employee, her personal information, including her name, employment information, Social Security Number, and date of birth were stolen in the November 2019 Breach. The letter also informed Cottrell that some breach victims' driver's license numbers were also compromised but it failed to inform Cottrell whether her driver's license number was among those affected. Cottrell received a letter substantially similar in all material respects to the letters attached hereto as Exhibits 1-3.

25. Because the Data Breach was an intentional hack by cyber criminals seeking information of value that they could exploit, Plaintiff Cottrell is at imminent and substantial risk of identity theft that is continuous and ongoing.

26. Cottrell has already had to spend time responding to the Data Breach, including time spent monitoring her accounts, obtaining credit monitoring, and otherwise attempting to mitigate the harms of the Breach. Due to the permanent and sensitive nature of some of the PII exposed in the Breach (such as Social Security Numbers), Cottrell will be required to continuously monitor her identity and credit for the rest of her life.

27. To Cottrell's knowledge, she has not been the victim of any other data breach.

28. Cottrell is very worried about the significant risk of identity theft she now faces.

Plaintiff Edward Hellyer

29. Plaintiff Edward Hellyer is domiciled in and a citizen of Citrus County, Florida.

30. Hellyer retired from Cablevision/Altice in 2017, after a 35-year career with the company in New York. He moved to Florida in 2018.

31. As part of his employment, Hellyer was required to provide Altice with his PII, including the information compromised in the Data Breach. Through his employment, he was also a subscriber of Altice's cable TV service. To subscribe, he was required to provide Altice with his PII, including some of the information compromised in the Data Breach.

32. On February 10, 2020, a breach notice letter, addressed to Plaintiff Hellyer, was delivered to his brother's house. The letter informed Hellyer that, as a former employee, his personal information, including name, employment information, Social Security Number, and date of birth were stolen in the November 2019 Breach. Altice informed Hellyer that some breach victims' driver's license numbers were also compromised, but Altice failed to inform Hellyer whether his driver's license number was among those affected. A copy of the letter sent to Hellyer is attached hereto as Exhibit 1.

33. Because the Data Breach was an intentional hack by cyber criminals seeking information of value that they could exploit, Plaintiff Hellyer is at imminent and substantial risk of identity theft that is continuous and ongoing.

34. Hellyer has already had to spend time responding to the Data Breach, including checking credit reports, verifying credit freezes, and reviewing resources on identitytheft.gov regarding how to protect himself from identity theft. Due to the permanent and sensitive nature of some of the PII exposed in the Breach (such as Social Security Numbers), Hellyer will be required to continuously monitor his identity and credit for the rest of his life.

35. Hellyer expects to pay for identity theft monitoring protection for the rest of his life because identity thieves have his PII.

36. To Hellyer's knowledge, he has not been the victim of any other data breach.

Plaintiff Carrie Mason-Draffen

37. Plaintiff Carrie Mason-Draffen is domiciled in and a citizen of Nassau County, New York.

38. Mason-Draffen was an employee of Newsday from 1984 to 2019, including during the period from 2016 to 2018 when Altice owned Newsday.

39. As part of her employment with Newsday/Cablevision, Mason-Draffen was required to provide Newsday/Cablevision with her PII, including the information compromised in the Data Breach. For many years of her employment with Newsday/Cablevision, she was also a subscriber of Optimum cable TV service. To subscribe, she was required to provide Altice with her PII, including some of the information compromised in the Data Breach. She is still a subscriber with Altice's Optimum cable TV service.

40. On February 10, 2020, she received a breach notification letter from Altice stating that, as a former employee, her personal information, including name, employment information, Social Security Number, and date of birth were stolen in the November 2019 Breach. Altice informed Mason-Draffen that some breach victims' driver's license numbers were also compromised but Altice failed to inform Mason-Draffen whether her driver's license number was among those affected. Mason-Draffen received a letter substantially similar in all material respects to the letters attached hereto as Exhibits 1-3.

41. As evident from the breach notification letter she received, Altice did not destroy Mason-Draffen's PII when it sold Newsday, but retained copies of it and all other Newsday employees' PII on the unencrypted document that was accessed and downloaded in the Breach.

Mason-Draffen is concerned that Altice still retains her information even after divesting itself of all interest in Newsday.

42. Because the Data Breach was an intentional hack by cyber criminals seeking information of value that they could exploit, Plaintiff Mason-Draffen is at imminent and substantial risk of identity theft that is continuous and ongoing.

43. Mason-Draffen has already had to spend time responding to the Data Breach, including checking her accounts and credit reports. Due to the permanent and sensitive nature of some of the PII exposed in the Breach (such as Social Security Numbers), Mason-Draffen will be required to continuously monitor her identity and credit for the rest of her life.

44. To Mason-Draffen's knowledge, the PII compromised in this Data Breach has never been compromised in any other data breach. She is very worried about the significant risk of identity theft she now faces.

Plaintiff Haseeb Raja

45. Plaintiff Haseeb Raja is domiciled in and a citizen of Kings County, New York

46. Plaintiff was employed by Altice from March 2008 to December 2019.

47. As part of his employment with Altice, Raja was required to provide Newsday/Cablevision with his PII, including the information compromised in the Data Breach. Through his employment with Altice, he was also a subscriber of Altice's Optimum cable TV service. To subscribe, he was required to provide Altice with his PII, including some of the information compromised in the Data Breach. He is still a subscriber with Altice's Optimum cable TV service.

48. On February 9, 2020, Raja received a Breach notification letter from Altice stating that, as a former employee, his personal information, including name, employment information,

Social Security Number, and date of birth were stolen in the Data Breach. Altice informed Raja that some Breach victims' driver's license numbers were also compromised but Altice failed to inform Raja whether his driver's license number was among those affected. A copy of the letter Raja received is attached hereto as Exhibit 2.

49. Because the Data Breach was an intentional hack by cyber criminals seeking information of value that they could exploit, Plaintiff Raja is at imminent and substantial risk of identity theft that is continuous and ongoing.

50. Raja has spent time responding to the Data Breach and will be required to continuously monitor his identity and credit for the rest of his life. Indeed, Raja has spent over 3 hours so far responding to the Data Breach, including time spent monitoring accounts, changing passwords, and obtaining credit monitoring. Raja anticipates having to spend significantly more time in the future. Indeed, due to the permanent and sensitive nature of some of the PII exposed in the Breach (such as Social Security Numbers), Raja will be required to continuously monitor his identity and credit for the rest of his life.

51. Because his information is in the hands of identity thieves from this Data Breach, Raja expects to pay for identity theft protection and credit monitoring going forward indefinitely, at great expense.

52. To Raja's knowledge, he has never been the victim of any other data breach.

Plaintiff Ronnie Gill

53. Plaintiff Ronnie Gill is domiciled in and a citizen of Suffolk County, New York.

54. Gill retired from Newsday in June 2019 after a forty-seven year career with the company. She was a Newsday employee during the period from 2016 to 2018 when Altice owned Newsday.

55. As part of her employment with Newsday, Gill was required to provide Newsday her PII, including the information compromised in the Data Breach. Gill was an Optimum cable TV subscriber, which required her to provide her PII, including some of the information compromised in the Data Breach. She canceled her Optimum cable TV subscription in 2011.

56. On February 11, 2020, Gill received a breach notification letter from Altice stating that, as a former employee, her personal information, including name, employment information, Social Security Number, and date of birth were stolen in the November 2019 Data Breach. Altice informed Gill that some breach victims' driver's license numbers were also compromised but Altice failed to inform Gill whether her driver's license number was among those affected. A copy of the letter that Gill received is attached hereto as Exhibit 3.

57. As evident from the breach notification letter she received, even after having sold Newsday, Altice did not destroy Gill's PII but retained copies of it and other Newsday employees' PII on the unencrypted report that was accessed and downloaded in the Breach. Gill was shocked and upset to learn that Altice still retained her PII and that of other Newsday employees on Altice's company servers and in an unencrypted report in its email accounts two years after Altice had completely divested itself of Newsday.

58. Because the Data Breach was an intentional hack by cyber criminals seeking information of value that they could exploit, Gill is at imminent and substantial risk of identity theft that is continuous and ongoing.

59. Gill has already had to spend several hours responding to the Data Breach, including contacting her financial institutions, changing notification settings on her accounts to trigger emails for suspicious activity, contacting her financial manager to increase the security of her investment account, obtaining credit monitoring, and periodically scrutinizing her transactions

and credit reports. Due to the permanent and sensitive nature of some of the PII exposed in the Breach (such as Social Security Numbers), Gill will be required to continuously monitor her identity and credit for the rest of her life.

60. To Gill's knowledge, the PII compromised in this Data Breach has never been compromised in any other data breach. Gill is very concerned about the jeopardy Altice has placed her in and is worried that she will forever be at greatly increased risk of identity theft.

Plaintiff John Frontera

61. Plaintiff John Frontera is domiciled in and a citizen of Suffolk County, New York.

62. Frontera worked for Cablevision/Altice over 30 years, retiring in April 2017.

63. As part of his employment with Cablevision/Altice, Frontera was required to provide Cablevision with his PII, including the information compromised in the Data Breach. Through his employment with Altice, he was also a subscriber of Altice's Optimum cable TV service. To subscribe, he was required to provide Altice with his PII, including some of the information compromised in the Data Breach. He is still a subscriber with Altice's Optimum cable TV service.

64. On February 12, 2020, Frontera received a breach notification letter from Altice stating that, as a former employee, his personal information, including name, employment information, Social Security Number, and date of birth were stolen in the Data Breach. Altice also informed Frontera that some breach victims' driver's license numbers were also compromised, but Altice failed to inform Frontera whether his driver's license number was among those affected. Frontera received a letter substantially similar in all material respects to the letters attached hereto as Exhibits 1-3.

65. Because the Data Breach was an intentional hack by cyber criminals seeking information of value that they could exploit, Frontera is at imminent and substantial risk of identity theft that is continuous and ongoing.

66. Frontera has already had to spend several hours responding to the Data Breach, including reviewing his credit reports, placing fraud alters and credit freezes with the Credit Bureaus, setting up an IRS pin, frequently checking his online banking and credit card accounts, and otherwise attempting to protect himself from identity theft. Due to the permanent and sensitive nature of some of the PII exposed in the Breach (such as Social Security Numbers), Frontera will be required to continuously monitor his identity and credit for the rest of his life.

67. Because his information is in the hands of identity thieves from this Data Breach, Frontera expects to pay for identity theft protection and credit monitoring going forward indefinitely, at great expense.

68. To his knowledge, Frontera has not been the victim of any other data breach.

Plaintiff Shariq Mehfooz

69. Plaintiff Shariq Mehfooz is domiciled in and a citizen of Suffolk County, New York.

70. Mehfooz was employed by Altice from September 2012 to March 2017, working at the Jericho and Bethpage Cablevision locations.

71. As a part of his employment with Cablevision/Altice, Mehfooz was required to provide Altice with his PII, including the information compromised in the Data Breach. Through his employment with Altice, he was also a subscriber of Altice's Optimum cable TV service. To subscribe, he was required to provide Altice with his PII, including some of the information compromised in the Data Breach. He is still a subscriber with Altice's Optimum cable TV service.

72. In February 2020, Mehfooz received a breach notification letter from Altice stating that, as a former employee, his personal information, including his name, employment information, Social Security Number, and date of birth were stolen in the Data Breach. Altice also informed Mehfooz that some breach victims' driver's license numbers were also compromised, but Altice failed to inform Mehfooz whether his driver's license number was among those affected. Mehfooz received a letter substantially similar in all material respects to the letters attached hereto as Exhibits 1-3.

73. In March 2020, Mehfooz was in the process of applying to refinance his home to take advantage of the low mortgage rates. On March 23, 2020, Mehfooz discovered that someone had opened an unauthorized credit card in his name through Merrick Bank. This new, fraudulent credit card application harmed his credit score and interrupted the refinancing process.

74. The identity theft resulting from the Data Breach contributed to Mehfooz having to suspend his attempt to refinance his home mortgage. Mehfooz is continuing to pay more each month than he would if he refinanced his home and he may miss out on the historically low interest rates.

75. Mehfooz has spent several days responding to the identity theft, including attempting to restore his identity and credit, placing phone calls with the credit bureaus, corresponding with Merrick Bank to close the fraudulent account, participating in additional phone calls and correspondence with his mortgage lender, obtaining credit monitoring, placing freezes on his credit reports, registering on identitytheft.gov, and otherwise attempting to protect himself and mitigate the harms caused by the Breach.

76. Due to the permanent and sensitive nature of some of the PII exposed in the Breach (such as Social Security Numbers), Mehfooz will be required to continuously monitor his identity and credit for the rest of his life.

77. Because the Data Breach was an intentional hack by cyber criminals seeking information of value that they could exploit, Mehfooz is at imminent and substantial risk of further identity theft that is continuous and ongoing.

78. Mehfooz has experienced considerable distress and anxiety as a result of the Breach.

79. Mehfooz has never before been a victim of identity theft. To his knowledge, the PII compromised in this Data Breach has never been compromised in any prior data breach.

Plaintiff Steven Paniccia

80. Plaintiff Steven Paniccia is domiciled in and a citizen of Nassau County, New York.

81. Paniccia was employed by Altice from May 2016 to February 2020.

82. As a part of his employment with Altice, Paniccia was required to provide Altice with his PII, including the information compromised in the Data Breach. Paniccia was also a subscriber of Altice's Optimum cable TV service. To subscribe, he was required to provide Altice with his PII, including some of the information compromised in the Data Breach.

83. In February 2020, Paniccia received a breach notification letter from Altice stating that, as a former employee, his personal information, including his name, employment information, Social Security Number, and date of birth were stolen in the Data Breach. Altice also informed Paniccia that some breach victims' driver's license numbers were also compromised, but Altice failed to inform Paniccia whether his driver's license number was among those affected. Paniccia

received a letter substantially similar in all material respects to the letters attached hereto as Exhibits 1-3.

84. In mid-December 2019, just one month after the Data Breach, Paniccia discovered that someone was using his PII to fraudulently open a credit card in his name.

85. Paniccia has spent several hours responding to the Data Breach and identity theft, including cancelling the fraudulent credit card, closely monitoring his financial accounts, monitoring all financial transactions, reviewing his credit monitoring reports, reviewing emails for suspicious activity, and otherwise attempting to protect himself and mitigate the harms caused by the Breach.

86. Due to the permanent and sensitive nature of some of the PII exposed in the Breach (such as Social Security Numbers), Paniccia will be required to continuously monitor his identity and credit for the rest of his life.

87. Because the Data Breach was an intentional hack by cyber criminals seeking information of value that they could exploit, Paniccia is at imminent and substantial risk of further identity theft that is continuous and ongoing.

88. To his knowledge, Paniccia has not been a victim of any other data breach.

Defendant Altice USA, Inc.

89. Defendant Altice USA, Inc. is incorporated in the State of Delaware and its principal place of business is Long Island City, New York.

90. Altice, with its subsidiaries, provides broadband communications and video services in the United States. It is the fourth largest cable provider in the U.S., operating under, among other brands, Altice, Optimum, Lightpath, and Suddenlink. It provides cable services to customers in 21 states, including those in the Tri-State area and south-central regions of the U.S.,

providing broadband, pay television, telephony services, proprietary content and advertising services. It was formed as the result of acquisitions by Altice N.V., a multinational telecommunications company centered in Europe, including of Suddenlink Communications, Cablevision, Newsday, and various other companies.

III. JURISDICTION AND VENUE

91. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

92. This Court has personal jurisdiction over Defendant because its principal place of business is in this State, it regularly transacts business in this District, and Plaintiff McFarlane and many Class Members reside in this District. Venue is likewise proper as to Defendant in this District because Defendant employed Plaintiff McFarlane in this District, employs a significant number of Class Members in this District, Plaintiff McFarlane was cable subscribers in this District along with a substantial number of the Subscriber Subclass, and a substantial part of the events or omissions giving rise to the claim occurred in this District. 28 U.S.C. § 1391(b)(2).

IV. FACTUAL ALLEGATIONS

A. The Data Breach

93. Sometime in the fall of 2019, cyber criminals decided that Altice had weak cyber security and was ripe for a phishing attack. Accordingly, these hackers initiated a phishing campaign against Altice.

94. Phishing attacks are common, and most companies avoid falling victim to them by a combination of email protection software, regular employee anti-phishing trainings, and other

basic cybersecurity precautions. Altice was grossly negligent and disregarded the obvious and substantial risks of such an attack.

95. In November 2019, the untrained and ill-equipped workers at Altice were attacked with a phishing campaign. The notice letters Altice sent explain that *multiple* Altice email accounts fell into the hands of cyber criminals, including, apparently, some high-level employees in positions of trust to whom Altice provided access to a highly sensitive yet unencrypted report containing the PII of 52,846 individuals.

96. State data breach laws require that in the case of a data breach, businesses are to send notice letters to all affected individuals, explaining what happened and what information was compromised in the data breach. *See, e.g.*, N.Y. Gen. Bus. Law § 899-aa. Some states publish the notice letters on their attorney general's website to provide additional notice to breach victims and the public. The example notice letter Altice provided to the Vermont Attorney General (the "Notice Template")[4] put it this way:

> **What happened?**
>
> In November 2019, an unauthorized third party gained access to certain Altice USA employees' email account credentials through a phishing incident. The unauthorized third party then used the stolen credentials to remotely access and, in some instances, download the employees' mailbox contents. . . .
>
> **What information was involved?**
>
> During our investigation, we learned in January 2020 that one of the downloaded mailboxes contained a password protected report that contained personal information, including name, employment information, Social Security number, date of birth and, in some instances, drivers' license number.

[4] *See* Altice USA Inc Notice of Data Breach to Consumers, OFFICE OF VERMONT ATTORNEY GENERAL (Feb. 6, 2020), https://ago.vermont.gov/blog/2020/02/06/altice-usa-inc-notice-of-data-breach-to-consumers/ (the "Vermont Notice").

97. The Notice Template then included alternative text block that stated either: "As a current employee, your personal information was included in this report." Or "As a former employee, your personal information was included in this report."[5]

98. An Altice spokesperson admitted that the unencrypted report contained the PII, including Social Security numbers, of all current employees.[6]

99. From the alternative "[a]s a former employee" option in the Notice Template, it is also apparent that this unencrypted report contained the PII of numerous former employees as well.

100. While the Notice also states that Defendant has "no information at this time that would indicate that your personal information has been misused,"[7] this disregards the obvious misuse caused by the fact that the cyber criminals had already *downloaded* Plaintiffs' and Class Members' personal information.

101. News reporting on the Data Breach has provided additional details. In an article published on February 11, 2020, Newsday reported that the cyber criminals were able to steal the PII of "all 12,000 current employees."[8]

102. Altice has admitted elsewhere that a total of 52,846 individuals had their information accessed and downloaded in the Data Breach.[9]

---

[5] *Id.*

[6] James T. Madore, *Data breach exposes Altice employee, Optimum customer information*, NEWSDAY (Feb. 11, 2020 4:32 PM), https://www.newsday.com/business/altice-data-breach-employees-Subscribers-1.41718432.

[7] Vermont Notice, *supra*.

[8] James T. Madore, *Data breach exposes Altice employee, Optimum customer information*, NEWSDAY (Feb. 11, 2020 4:32 PM), https://www.newsday.com/business/altice-data-breach-employees-Subscribers-1.41718432.

[9] *See* "Data Breach Year-to-date Report April 2020," Indiana Attorney General, https://www.in.gov/attorneygeneral/files/Data%20Breach%20Year-to-date%20Report%20April%202020.pdf.

103. Altice failed to take the necessary precautions required to safeguard and protect Plaintiffs' and the other Class Members' PII from unauthorized disclosure. Defendant's actions represent a flagrant disregard of its employees' and subscribers' rights, both as to privacy and property.

104. Employees were required by Altice to provide their sensitive PII, including their Social Security Numbers, as a condition of their employment.

105. Subscribers too, including employee subscribers, were required to provide confidential PII to Altice to obtain cable services such as television and internet.

B. Cyber Criminals Have Used and Will Continue to Use Plaintiffs' PII to Defraud Them

106. PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach can and will be used in a variety sordid ways for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

107. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[10] For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[11] These criminal

[10] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[11] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

activities have and will result in devastating financial and personal losses to Plaintiffs and the Class Members.

108. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[12]
>
> [Emphasis added.]

109. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[13]

110. This was a financially motivated Breach, as the only reason the cyber criminals go through the trouble of running a targeted phishing campaign against companies like Altice is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein, particularly in paragraph 107. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[14] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[15]

---

[12] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[13] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[14] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[15] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

111. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, they ***will*** use it.[16]

112. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

113. For instance, with a stolen social security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[18]

114. With this Data Breach, and as demonstrated by the identity theft Plaintiffs McFarlane, Mehfooz, and Paniccia and other Class Members have already experienced, identity thieves have already started to prey on the Altice breach victims, and we can anticipate that this will continue.

115. Identity theft victims like Plaintiffs McFarlane, Mehfooz, and Paniccia as well as other Class Members, must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[19]

---

[16] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[17] *Data Breaches Are Frequent*, *supra* note 11.

[18] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[19] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

116. Defendant's offer of one year of identity monitoring to Plaintiffs and the Class is woefully inadequate and will not fully protect Plaintiffs from the damages and harm caused by its failures. While some harm has begun already, as several Plaintiffs have already found out, the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. Once the twelve-months have expired, Plaintiffs and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Altice's gross negligence. Furthermore, identity monitoring only alerts someone to the fact that they have *already been the victim of identity theft* (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.[20] Nor can an identity monitoring service remove personal information from the dark web.[21] "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[22]

117. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have suffered actual identity theft, have been damaged, and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial

[20] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

[21] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[22] *Id.*

accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiffs McFarlane, Mehfooz, and Paniccia and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiffs and the Class must take.

118. Plaintiffs and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;
b. Trespass, damage to, and theft of their personal property including PII;
c. Improper disclosure of their PII;
d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and having been already misused;
e. Damages flowing from Defendant's untimely and inadequate notification of the data breach, including the uncertainty of whether they need to replace their driver's licenses;
f. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII and that identity thieves have already used that information to defraud other victims of the Data Breach;
g. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

h. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

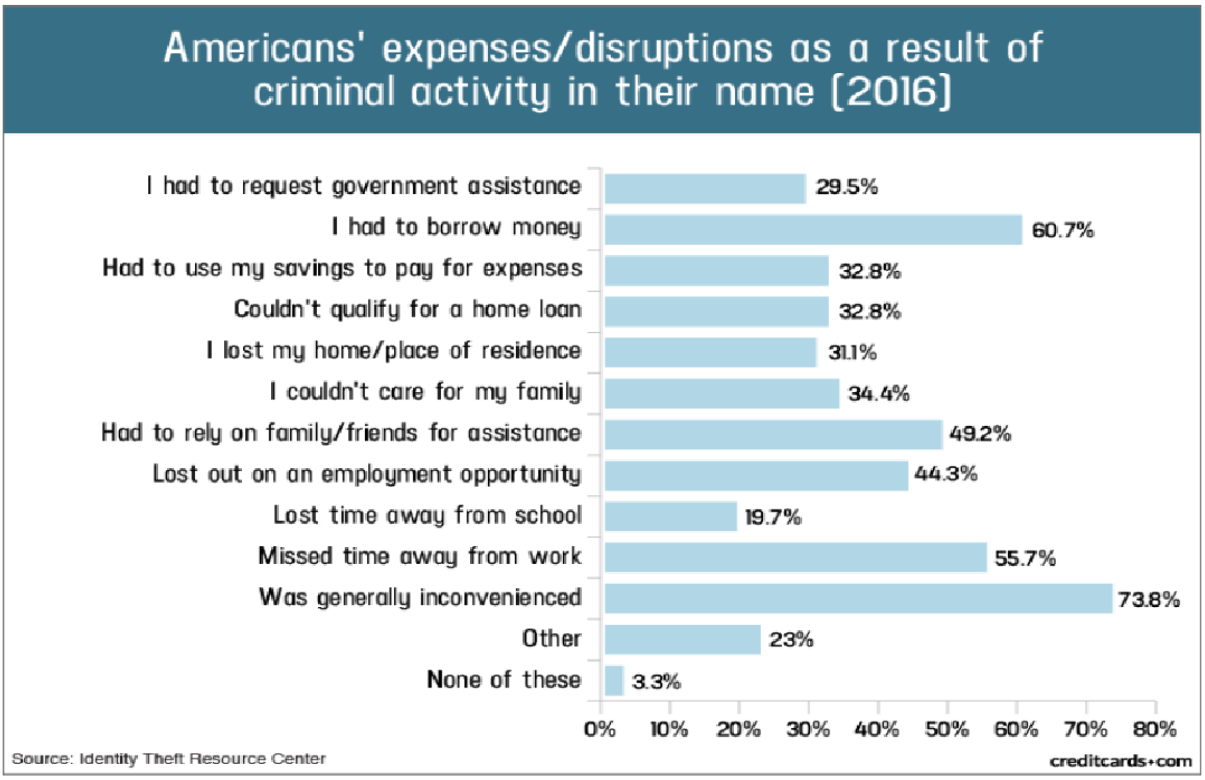
i. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class members' personal information for which there is a well-established and quantifiable national and international market;

j. The loss of use of and access to their credit, accounts, and/or funds;

k. Damage to their credit due to fraudulent use of their PII; and

l. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

119. Below is a chart that shows the kinds of expenses and disruptions that victims of identity theft experience[23]:



[23] Jason Steele, *Credit Card and ID Theft Statistics*, CREDITCARDS.COM (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

120. Moreover, Plaintiffs and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiffs' PII.

121. Plaintiffs Mason-Draffen and Gill from Newsday also have an interest in ensuring that their information and that of all other current and former Newsday employees is destroyed from all Altice servers, and especially from Altice's unencrypted company email accounts.

122. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiffs and Class Members the woefully inadequate twelve months of identity theft repair and monitoring services. Twelve months of identity theft and repair and monitoring is, however, inadequate to protect Plaintiffs and Class Members from a lifetime of identity theft risk.

123. Defendant further acknowledged, in its letter to Plaintiffs and other Class Members, that Altice needed to improve its security protocols, stating:

> [W]e continue taking steps to prevent similar situations from happening in the future, including:
>
> - having reset passwords for all compromised accounts to prevent further unauthorized access;
> - conducting additional *mandatory education to help employees recognize and avoid phishing emails*;
> - *revising internal policies and practices to strengthen our internal security standards*; and
> - *strengthening email system security controls and protocols*.

124. The letter further acknowledged that the Data Breach would cause inconvenience to affected individuals and that financial harm would likely occur, stating:

> Please review the enclosed "Additional Resources" document which describes *additional steps you can take to help protect yourself, including recommendations*

> *by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit line.*
>
> ***
>
> *We regret any inconvenience or concern this may have caused* and are continuing to take steps to demonstrate our ongoing commitment to the security of your information.

125. At Altice's suggestion, Plaintiffs are desperately trying to mitigate the damage that Altice has caused them. Given the kind of PII Altice made accessible to hackers, however, Plaintiffs are certain to incur additional damages. Because identity thieves have their PII, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[24]

126. None of this should have happened.

C. Defendant was Aware of the Risk of Cyber-Attacks

127. Data security breaches from phishing campaigns have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest phishing-related data breaches: Target,[25] Yahoo,[26]

[24] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

[25] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[26] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

Marriott International,[27] Chipotle, Chili's, Arby's,[28] and others.[29]

128. As one of the largest cable TV and communications providers in the United States, with nearly 5 million subscribers across 21, Altice should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the PII that it collected and maintained.

129. As a New York employer, New York law requires that Altice protect its employees' Social Security Numbers, and requires that Altice notify its employees of that law. *See* N.Y. Labor Law § 203-d(1) and (3). Altice knowingly violated this statute and its other duties when it cut costs and eliminated and/or failed to put in place policies or procedures to safeguard against unauthorized disclosure.

130. Further, because Altice provided, as a benefit of employment, discounted cable services to its employees, Altice was further aware that its failure to establish and maintain industry standard data security technologies and practices to secure its employees' PII could likely result in violations of the Cable Communications Act of 1984 ("Cable Act"), 47 U.S.C. § 551, *et seq.*

131. Indeed, in its Customer Privacy Notice to subscribers, Altice acknowledges that it is a "cable operator" under the Cable Act and that as a cable operator, it owes special statutory duties to its subscribers to protect their PII from unauthorized disclosure, stating:

> The Cable Act imposes limitations with respect to the collection and disclosure of personally identifiable information by cable operators . . . . [C]able operators generally may not disclose personally identifiable information without consent of

[27] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[28] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[29] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

> the subscriber concerned. Also, cable operators ***must take such actions as are necessary to prevent unauthorized access to such information*** by a person other than the subscriber or cable operator. If we violate your rights, you may be entitled to bring a civil action in a federal court, which may award actual, liquidated, and punitive damages, fees and costs, and other remedies that may be available.[30]
>
> [Emphasis added.]

132. Thus, in its Customer Privacy Notice, Altice represented to subscribers, including employees who were subscribers, the following:

> We employ physical, electronic, and procedural safeguards to protect Subscriber Information. For example, we utilize secure socket layer (SSL) encryption to protect certain information you provide to us; employ verification measures to protect e-mail during delivery; maintain certain subscriber databases in restricted areas; and secure the content by use of firewalls and other security methods. We also limit access to databases containing subscribers' Personally Identifiable Information to specifically authorized employees and agents and other parties identified in the disclosure section above.[31]

133. Had Altice done as it promised and as it was obligated under the law, the Data Breach would not have happened and Plaintiffs and Class Members would not have been damaged.

134. Altice's awareness of the risks of a cyberattack was on wide display in the weeks immediately following its mailing of the Data Breach notification letters. As Plaintiffs and Class Members were scrambling to respond to the Data Breach, Altice ran a tone-deaf television advertisement bragging about its advanced cybersecurity capabilities (the "Ad").

135. In the Ad, a man walks into a veterinarian office and asks for his pet named "Muffin." The office staff nervously greet the man and bring him a Pomeranian stating, "Here's Muffin." "This isn't Muffin," says the man. "Are you sure?" the receptionist hesitantly asks. "Muffin's a rabbit," responds the man. The office staff then fess-up. "Okay, we got hacked. We

---

[30] Customer Privacy Notice (effective Oct. 15, 2018), https://www.optimum.net/pages/PrivacyExisting.html.

[31] *Id.*

lost all of our data." The receptionist then jokingly adds, "I guess they don't call it '*free*' antivirus software for nothing, right?" The Ad copy then reads, "Unsafe Internet can cost you your business." The Ad goes on to claim that Altice's Optimum business internet service protects against various cyber threats, *including phishing*.

136. In its internet security software advertisements, Altice Optimum similarly assures: "Protecting you and your family online is a top priority for us."[32]

137. Given Altice's representation of itself as meeting a higher standard of cybersecurity, the Court should hold Altice to this heightened standard. Altice's repeated assurances certainly make it evident that Altice recognized it had a duty to use reasonable measures to protect the PII that it collected and maintained.

138. Additionally, over a year before the Data Breach, Altice stated the following in its Form 10-K filed with the Securities and Exchange Commission:

> *Privacy and Data Security.* In the course of providing our services, we collect certain information about our customers and their use of our services. We also collect certain information regarding potential customers and other individuals. Our collection, use, disclosure and other handling of information is subject to a variety of federal and state privacy requirements, including those imposed specifically on cable operators and telecommunications service providers by the Communications Act. We are also subject to data security obligations, as well as requirements to provide notice to individuals and governmental entities in the event of certain data security breaches, and such breaches, depending on their scope and consequences, may lead to litigation and enforcement actions with the potential of substantial monetary forfeitures or to adversely affect our brand.
>
> As cable operators provide interactive and other advanced services, additional privacy and data security requirements may arise through legislation, regulation or judicial decisions. . . .[33]

[32] *Internet Security*, OPTIMUM, https://www.optimum.net/pages/internet-protection.html.

[33] *Altice USA, Inc.* (NYSE: ATUS), Form 10-K at 14–15 (Mar. 6, 2018), https://www.sec.gov/Archives/edgar/data/1702780/000170278018000002/alticeusa12-31x1710xk.htm.

139. Altice was, therefore, clearly aware of the risks it was taking and the harm that could result.

D. Altice Was on Notice of the Inadequacy of Its Data Security and Altice's Disregard of Known and Substantial Risks Made the Data Breach Foreseeable

140. Prior to its acquisition by Altice, Suddenlink Communications had strict email mailbox retention policies, in which all email was automatically deleted after 90 days. Suddenlink also had tools in place, such as Proofpoint email security, to identify and filter out phishing emails and prevent business email compromise. Suddenlink also had regular, periodic cybersecurity training for employees which included training on phishing scams.

141. After Altice acquired Suddenlink, Altice eliminated many of the data security vendors and systems that provided security around the company networks to reduce costs. It also laid off many of the existing employees (who had benefitted from the periodic trainings) and increased its remaining employees' workloads.

142. Cablevision also spent more time and money on cybersecurity than Altice does. Prior to Altice's acquisition, Cablevision regularly trained and tested employees who had access to sensitive PII. Since acquiring Suddenlink and Cablevision, Altice has decreased spending across the board, including on essential cybersecurity. As part of this, Altice stopped requiring regular, periodic cybersecurity training for employees, instead emphasizing profit and productivity over training and security. Altice now only requires cybersecurity training when it releases new products.

143. Since Altice acquired Cablevision, Altice has also aggressively reduced the in-house workforce and has outsourced many critical operations to third parties, often requiring discounted rates and net-90 payment terms. This has resulted in a significant lack of adequate

cybersecurity staff, training, systems, and procedures, which facilitated the conditions that made the Data Breach possible.

144. Altice made a name for itself in aggressive cost-cutting and short-changing vendors. After acquiring Cablevision, Altice promised to "squeeze out an ambitious $900 million in cost savings from Cablevision."[34] At Suddenlink, following its acquisition, the purchase of a new office ice machine placed the office in the crosshairs of a corporate "investment committee," which, though staffed with executives, engaged in "a discussion at a very nitty-gritty level" for the purchase of this small, inexpensive office appliance.[35]

145. "I don't like to pay salaries . . . I pay as little as I can." This statement, by Altice NV founder Patrick Drahi, is part of Altice's ethos,[36] and it applies to vendors and suppliers as well, with the company "declar[ing] total war on channel carriage costs."[37] Among the vendors upon whom Altice has declared "total war" are those providing essential cybersecurity measures. Indeed, this cost-cutting has only grown in the last two years, with the shrinking of traditional cable television.[38]

---

[34] Nick Kostov & Shalini Ramachandran, *Altice's Big U.S. Cable Ambitions Begin With Austerity*, THE WALL STREET JOURNAL (Updated June 28, 2016, 11:01 am ET), https://www.wsj.com/articles/altice-will-rely-on-cost-cuts-to-make-cablevision-deal-work-1467123760?mod=article_inline.

[35] *Id.*

[36] Claire Atkinson, *Cablevision Workers Are Frustrated With Altice's Cutbacks*, NEW YORK POST (Dec. 14, 2016, 10:50 pm), https://nypost.com/2016/12/14/cablevision-workers-are-frustrated-with-altices-cutbacks/.

[37] Phillip Dampier, *Told You: Altice Brings Its Special Kind of Cost-Cutting to Suddenlink and Cablevision*, STOP THE CAP! (June 28, 2016), https://stopthecap.com/2016/06/28/told-altice-brings-special-kind-cost-cutting-suddenlink-cablevision/; *see also* Phillip Dampier, *Siren Song: Altice USA CEO Asks Workers to Trust Him Despite Ruthless Cost-cutting Reputation*, STOP THE CAP! (Jan. 4, 2017), https://stopthecap.com/2017/01/04/siren-song-altice-usa-ceo-asks-workers-trust-despite-ruthless-cost-cutting-reputation/ (noting Altice's critics often denounce it for "not paying vendors (or paying them only after they agree to provide discounts)").

[38] Lillian Rizzo & Drew FitzGerald, *Cord-Cutting Accelerated in 2019, Raising Pressure on Cable Providers*, THE WALL STREET JOURNAL (Updated Feb. 20, 2020, 6:15 am ET), https://www.wsj.com/articles/cord-cutting-accelerates-raising-pressure-on-cable-providers-11582149209?mod=searchresults&page=1&pos=4.

146. These actions by Altice facilitated the Data Breach and made it foreseeable.

E. Altice Could Have Prevented the Data Breach

147. Data breaches are preventable.[39] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[40] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[41]

148. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[42]

149. In a Data Breach like this, many failures laid the groundwork for the Breach. Indeed, email phishing attacks are one of the most common and preventable kinds of cyberattacks.[43]

150. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such

[39] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[40] *Id.* at 17.

[41] *Id.* at 28.

[42] *Id.*

[43] Safety Detectives, *The Ultimate Guide to Staying Safe from Phishing – 2020*, (Dec. 24, 2019), https://www.safetydetectives.com/blog/phishing-dangerous-yet-preventable-cyber-attacks/.

risks.[44] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

151. Upon information and belief, Altice failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Altice also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

152. Among other things, Altice's email protection software was not sufficient to recognize and block the phishing emails, even though multiple employees were receiving the same kind of emails at once (a red flag that would have been marked by good email protection systems).[45] Industry standard SPAM filters, DMARC enforcement, and/or Sender Policy Framework enforcement should have protected against these phishing emails.

---

[44] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[45] DuoCircle, *Protecting Your Business from Phishing Attacks*, Nov. 2, 2018, https://www.duocircle.com/phishing-protection/protecting-your-business-from-phishing-attacks.

153. In addition, Altice failed to require regular periodic anti-phishing and cybersecurity training for its employees, especially those in positions of trust dealing directly with employee and subscriber PII. It is well recognized that one of the best protections against email related threats is security awareness training and testing on a regular basis. This should be a key part of a company's on-going training of its employees. "[S]ince phishing is still a significant, initial point of compromise, additional work needs to be done to further lower the click rate. . . . This can be done through more frequent security awareness training, phishing simulation, and better monitoring of metrics pertaining to phishing (including whether there are any particular repeat offenders)."[46] Indeed, simply training employees to avoid the bait is one of the easiest ways to thwart a phishing campaign.[47] Altice clearly failed to train its employees to avoid falling victim to phishing emails, as evidenced by the fact that *multiple* Altice employees provided their login credentials to hackers during the successful phishing campaign.

154. Altice further had far too much confidential unencrypted information held in email accounts. Specifically, Altice permitted a document containing the unencrypted PII of *52,846* of its current and former employees and subscribers to not only be *sent* through email but to also remain *stored in* its company email accounts. None of this highly sensitive information should have been in an unencrypted report that was stored in Altice's accounts, but instead such PII should have been segregated into an encrypted system, separate from the email servers.[48]

---

[46] Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results*, PROOFPOINT (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishing-statistics-2019-himss-survey-results.

[47] Jennifer J. Daniels and Davide Oberly, *Employee Education, Training Is Key to Curtailing Risk of Phishing Attack*, May 24, 2019, https://www.propertycasualty360.com/2019/05/24/how-effective-employee-education-and-training-combats-phishing-attack-risk-414-155823/?slreturn=20200623160131.

[48] *See, e.g.*, Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

155. Moreover, it is well-established industry standard practice for a business to dispose of confidential PII once it is no longer needed. The FTC, among others, has repeatedly emphasized the importance of disposing unnecessary PII, saying simply: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[49] Altice, rather than following this basic standard of care, kept tens of thousands of former employees' unencrypted PII indefinitely. As a result, employees who left Altice several years earlier had their PII exposed in the Data Breach. This greatly expanded the number of victims harmed in the Breach.

156. In sum, this Data Breach could have readily been prevented through the use of industry standard email filtering software, regular awareness training for staff, proper network segmentation, and encryption of all confidential information. Further, the scope of the Data Breach could have been dramatically reduced had Altice utilized proper record retention and destruction practices.

157. As a large, publicly-traded company, with obligations to its tens of thousands of current and former employees and 5 million subscribers, Altice should have at least complied with the industry security standards for *small* businesses. But, as described below, it did not.

158. ProtonMail Technologies publishes a guide for IT Security to small businesses (*i.e.*, companies with far less PII to protect than Altice). In its 2019 guide, ProtonMail dedicates a full chapter of its ebook guide to the danger of phishing and ways a small business can avoid prevent falling prey to a phishing attack. It acknowledged the prevalence of the problem and the best defense against it:

[49] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf at p. 6.

> [Y]our email security relies on training your employees to implement security best practices and to recognize possible phishing attempts. This must be deeply ingrained into every staff member so that every time they check their emails, they are alert to the possibility of malicious action.[50]

159. The guidance that ProtonMail provides small businesses is likely necessary but not sufficient for a company like of Altice, with its added obligations under the heightened standard of the New York Labor Law, the Cable Communications Act of 1984, and the increased danger from the sensitivity and sheer volume of PII that Altice retains. But ProtonMail's guidance nevertheless illustrates just how inadequate Altice's security measures were. ProtonMail lists numerous tools under the heading, "How to Prevent Phishing," including:

a. **Training:** "Training your employees on how to recognize phishing emails and what to do when they encounter one is the first and most important step in maintaining email security. *This training should be continuous* . . . ."

b. **Limit Public Information:** "Attackers cannot target your employees if they don't know their email addresses. Don't publish non-essential contact details on your website or any public directories . . . .

c. **Carefully check emails:** "First off, your employees should be skeptical anytime they receive an email from an unknown sender. Second, most phishing emails are riddled with typos, odd syntax, or stilted language. Finally, check the 'From' address to see if it is odd . . . . If an email looks suspicious, employees should report it."

d. **Beware of links and attachments:** "Do not click on links or download attachments without verifying the source first and establishing the legitimacy of the link or attachment. . . ."

[50] *The ProtonMail Guide to IT Security for Small Businesses*, PROTONMAIL (2019), available at https://protonmail.com/it-security-complete-guide-for-businesses.

e. **Do not automatically download remote content:** "Remote content in emails, like photos, can run scripts on your computer that you are not expecting, and advanced hackers can hide malicious code in them. You should configure your email service provider to not automatically download remote content. This will allow you to verify an email is legitimate before you run any unknown scripts contained in it."

f. **Hover over hyperlinks:** "Never click on hyperlinked text without hovering your cursor over the link first to check the destination URL, which should appear in the lower corner of your window. Sometimes the hacker might disguise a malicious link as a short URL."

g. **If in doubt, investigate:** "Often phishing emails will try to create a false sense of urgency by saying something requires your immediate action. However, if your employees are not sure if an email is genuine, they should not be afraid to take extra time to verify the email. This might include asking a colleague, your IT security lead, looking up the website of the service the email is purportedly from, or, if they have a phone number, calling the institution, colleague, or client that sent the email."

h. **Take preventative measures:** "Using an *end-to-end encrypted email service* gives your business's emails an added layer of protection in the case of a data breach. A spam filter will remove the numerous random emails that you might receive, making it more difficult for a phishing attack to get through. Finally, other tools, like Domain-based Message Authentication, Reporting, and Conformance (DMARC) help you be sure that the email came from the person it claims to come from, making it easier to identify potential phishing attacks."[51]

[51] *Id.*

160. These are basic, common-sense email security measures that every business, especially large, publicly traded businesses, should have implemented long ago. Altice, with its heightened duties under New York Labor Law, the Cable Communication Act, and SOX should have done more. By taking these commonsense solutions, Altice could have prevented this Data Breach from occurring.

F. Altice's Use of a Single Password Was Woefully Insufficient to Secure Sensitive PII

161. Altice's letter to Plaintiffs and Class Members indicates that report that was accessed and downloaded by hacker was "password protected."[52] However, Altice's use of a single password on a document containing the unencrypted highly sensitive and valuable personal information of 52,846 people was wholly inadequate and was certainly no substitute for the industry standard security measures discussed in the immediately preceding section.

162. As an initial matter, when a password-protected document is sent by email, it is often the case that the password for the document is contained within the same mailbox or even in the very same email as the password-protected document.[53] Thus, the unauthorized hacker may well have obtained the password within the files it downloaded from Altice's corporate accounts.

163. Even if the password was not also obtained by the hacker, the fact remains that a password-protected document can *easily* be opened even by an average layperson using readily

[52] *See* Altice USA Inc Notice of Data Breach to Consumers, Office of Vermont Attorney General (Feb. 6, 2020), https://ago.vermont.gov/blog/2020/02/06/altice-usa-inc-notice-of-data-breach-to-consumers/.

[53] *How to Protect a PDF file, Document or Images with a Password*, https://digify.com/blog/protect-pdf-with-password/; *see also* Suzanne Kantra, *What to Do When Your Email Gets Hacked*, June 4, 2020, *https://www.techlicious.com/tip/what-to-do-when-your-email-gets-hacked/* (explaining that email boxes frequently contain numerous passwords that can be easily located with a search for "password"); Ponemon Institute LLC, *The 2019 State of Password and Authentication Security Behaviors Report*, Jan. 2019, https://www.yubico.com/wp-content/uploads/2019/01/Ponemon-Authentication-Report.pdf (survey showing that 26% of organizations store passwords in insecure files for employees to readily access them).

available internet tools.[54] "Cheap password-hacking utilities are available to anyone with the inclination and a few bucks."[55] In fact, there are several password removing or hacking tools that are available online completely free of charge.[56] "[P]assword protection remover tools were initially invented to be used only under appropriate circumstances – that is only if the original creator of the PDF file has lost the password and if the user has the legal right to view and modify the PDF but does not have the password. However as with all applications their use was quickly misused for gaining access to files by unauthorized users[.]"[57] Some of the most common tools operate to either recover the password, remove the password protection, or crack the password.[58] And in many instances, it is not even necessary to use these tools at all, as people can often entirely *bypass* the need for a password altogether by modifying features of the file or opening in other applications.[59] Accordingly, while "password protection seems to be a good idea because it's

[54] Elise Williams, *Best 5 Word Password Remover for You*, May 27, 2020 (describing tools that any person can use to open a password-protected document) https://pdf.wondershare.com/document-security/word-password-remover.html; *see also Unlock PDF Files* ("Not only are PDF password remover programs highly effective in easily decrypting PDF files, but many of them are available for free.") https://www.locklizard.com/remove-pdf-password-protection/.

[55] Susan Harkins, *10 Tips for Helping Users Keep Outlook Data Secure*, TECH REPUBLIC, Sept. 21, 2007, https://www.techrepublic.com/blog/10-things/10-tips-for-helping-users-keep-outlook-data-secure/.

[56] *Id.*; *see also* Henry Dalziel, *Password Cracking Tools for Use in 2020*, https://www.concise-courses.com/hacking-tools/password-crackers/ (describing several password hacking tools, including botnet powered tools, that can easily crack even complicated passwords within minutes).

[57] *Unlock PDF Files* ("Not only are PDF password remover programs highly effective in easily decrypting PDF files, but many of them are available for free.") https://www.locklizard.com/remove-pdf-password-protection/.

[58] Tim Fisher, *4 Best Free Tools for Recovering a Word Password*, Dec. 5, 2019 https://www.lifewire.com/free-word-password-recovery-tools-2626185; Amy Dennis, *How Can We Open a Password Protected Excel File?*, Jul. 18, 2020 https://recoverit.wondershare.com/office-document-repair/open-password-excel.html.

[59] Yousuf Hasan, *How to Open Password Protected PDF Without Password*, DATA RECOVERY SOLUTIONS, Mar. 1, 2019 https://www.data-recovery-solutions.com/blog/open-password-protected-pdf-without-password/.

easy, most implementations are not actually effective. That is fine if you just want to *appear* to have some security."[60]

164. The bottom line: a password-protected document is not a meaningful barrier to access, and it is certainly not a meaningful barrier to a cyber-criminal who has already invested considerable time in committing a phishing attack and then downloading files of interest, as was the case here. "A password only slows down a determined hacker[.]"[61] Indeed, because single passwords are so easily evaded by hackers, one technology writer has commented that "the only fans of passwords are hackers and identity thieves."[62]

G. Altice's Response to the Data Breach is Inadequate to Protect Plaintiffs and the Class

165. Altice failed to inform Plaintiffs and Class Members of the Data Breach in time for them to protect themselves from identity theft.

166. Altice stated that it discovered the Data Breach in November 2019. It did not disclose how long the cyber criminals had access to the Company accounts or the precise day when Altice discovered the Breach. The notice letters sent to Plaintiffs and Class Members stated that Altice did not learn of the existence of the Unencrypted Report until January 2020, two months after it discovered the Data Breach. And yet, Altice did not start notifying employees and affected subscribers until February 2020. Even then, Altice failed to inform Plaintiffs and Class Members whether or not their drivers' license numbers were exposed in the Data Breach, leaving Plaintiffs and Class Members unsure as to the scope of information that was compromised.

---

[60] *Unlock PDF Files* ("Not only are PDF password remover programs highly effective in easily decrypting PDF files, but many of them are available for free.") https://www.locklizard.com/remove-pdf-password-protection/.

[61] Susan Harkins, *10 Tips for Helping Users Keep Outlook Data Secure*, Tech Republic, Sept. 21, 2007, https://www.techrepublic.com/blog/10-things/10-tips-for-helping-users-keep-outlook-data-secure/.

[62] Jessica Guynn, *Dear Passwords: Forget You. Here's What is Going to Protect Us Instead*, USA Today, Feb. 28, 2020, https://www.usatoday.com/story/tech/2020/02/28/data-breaches-hackers-passwords/4870309002/.

167. During these intervals, the cyber criminals were exploiting the information while Altice was secretly still investigating the Data Breach. For example, while Alice was investigating the Breach, and had not notified its employees or subscribers, identity thieves had already begun applying for credit with the stolen names and Social Security Numbers of Breach Victims, including Plaintiffs McFarlane, Mehfooz, and Paniccia, who had credit cards opened in their names shortly after the Data Breach.

168. If Altice had investigated the Data Breach more diligently and reported it sooner, the damages could have been mitigated.

V. CLASS ACTION ALLEGATIONS

169. Plaintiffs incorporate by reference all preceding paragraphs as if fully restated here.

170. Plaintiffs bring this action against Altice on behalf of themselves and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of a nationwide class defined as follows:

> National Class
>
> All persons whose personally identifiable information was compromised as a result of the Data Breach at Altice USA, Inc. in November 2019.

171. Plaintiffs additionally assert claims on behalf of the following Subclasses:

> Employee Subclass
>
> All current and former employees whose personally identifiable information was compromised as a result of the Data Breach at Altice USA, Inc. in November 2019.[63]

[63] While it appears that the Data Breach may have only exposed the PII of current and former employees of Altice, because this is not known to Plaintiffs at this time, the Employee Subclass is alleged to clarify that the New York Labor Law claims are only raised on behalf of current and former employees.

Subscriber Subclass

> All current and former Altice (and related company) cable subscribers whose personally identifiable information was compromised as a result of the Data Breach at Altice in November 2019.

172. Excluded from the National Class and Subclasses are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

173. Plaintiffs reserve the right to amend the above definitions or to propose alternative or additional subclasses in subsequent pleadings and motions for class certification.

174. The National Class and Employee and Subscriber Subclasses are collectively referred to as the "Class" unless otherwise specified.

175. The proposed Class and subclasses meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

176. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Defendant has reported to the Indiana Attorney General's Office that the total number of individuals affected in the Data Breach was 52,846 individuals.[64]

177. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Altice's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Altice.

[64] *See* "Data Breach Year-to-date Report April 2020," Indiana Attorney General, https://www.in.gov/attorneygeneral/files/Data%20Breach%20Year-to-date%20Report%20April%202020.pdf.

178. **Adequacy:** Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the National Class and proposed Subclasses that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

179. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Altice's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

180. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

i. Whether Defendant engaged in the wrongful conduct alleged herein;

j. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's PII;

k. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their PII, and whether it breached this duty;

l. Whether Altice violated state and federal laws, thereby breaching its duties to Plaintiffs and the Class as a result of the Data Breach;

m. Whether Altice failed to provide adequate email security filtering;

n. Whether Altice failed to provide adequate anti-phishing training to its employees;

o. Whether Altice knew or should have known that its computer and network security systems were vulnerable to phishing attacks;

p. Whether Altice's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company email accounts;

q. Whether Altice was negligent in permitting an unencrypted report containing the PII off vast numbers of individuals to be stored within its unencrypted email accounts;

r. Whether Altice was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees;

s. Whether Altice breached implied contractual duties to Plaintiffs and the Class to use reasonable care in protecting their PII;

t. Whether Altice failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

u. Whether Altice continues to breach duties to Plaintiffs and the Class;

v. Whether Plaintiffs and the Class suffered injury as a proximate result of Altice's negligent actions or failures to act;

w. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief; and

x. Whether Altice's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of all Plaintiffs and the National Class)

181. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

182. Defendant Altice solicited, gathered, and stored the PII of Plaintiffs and the Class.

183. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed. Defendant had a duty to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiffs and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class Members had no ability to protect their PII that was in Altice's possession. As such, a special relationship existed between Altice and Plaintiffs and the Class.

184. Defendant was well aware of the fact that cyber criminals routinely target large corporations through phishing attacks and other cyberattacks in an attempt to steal employee and customer PII.

185. Defendant owed Plaintiffs and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when

obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

186. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts, including those in New York and the Second Circuit, and legislatures, including New York's, have recognized the existence of a specific duty owed by employers to reasonably safeguard the personal information of their employees.

187. Defendant had duties to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to phishing attacks, including by using adequate email filtering software, providing adequate and frequent training to employees on identifying, avoiding, and reporting suspicious emails; by using encrypted email accounts, by encrypting any document or report containing PII, by not permitting documents containing PII to be attached to or stored in emails, and other similarly common-sense precautions when dealing with sensitive PII. Additional duties that Altice owed Plaintiffs and the Class include:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;
b. To protect the PII in its possession using reasonable and adequate security procedures and systems;
c. To adequately and properly audit, test, and train its employees to avoid phishing emails;

d. To use adequate email security systems, including industry standard SPAM filters, DMARC enforcement, and/or Sender Policy Framework enforcement, to protect against phishing emails;

e. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

f. To train its employees not to store PII in their email inboxes longer than absolutely necessary for the specific purpose that it was sent or received;

g. To implement processes to quickly detect a data breach, security incident, or intrusion; and

h. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

188. Plaintiffs and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Altice. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiffs and the Class had entrusted to it.

189. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees to avoid phishing emails;

d. Failing to use adequate email security systems, including industry standard SPAM filters, DMARC enforcement, and/or Sender Policy Framework enforcement, to protect against phishing emails;

e. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

f. Failing to adequately and properly train its employees not to store PII in their email inboxes, and certainly not longer than absolutely necessary for the specific purpose that it was sent or received;

g. Failing to consistently enforce security policies aimed at protecting Plaintiffs and the Class's PII;

h. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

i. Failing to abide by reasonable retention and destruction policies for PII of former employees; and

j. Failing to promptly and accurately notify Plaintiffs and Class Members of the Data Breach that affected their PII, *see* N.Y. Gen. Bus. Law § 899-aa(2), (4).

190. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

191. By deliberately canceling necessary anti-phishing trainings and security contracts and attaching and storing an unencrypted report containing the highly sensitive PII of 52,846 individuals on its unencrypted email, Defendant intentionally engaged in unreasonable conduct in reckless disregard of a known or obvious risk that was so great as to make it highly probable that

harm would follow. Defendant engaged in these egregious acts with conscious indifference to the readily foreseeable and predictable outcome.

192. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

193. The damages Plaintiffs and the Class have suffered (as alleged above) were and are reasonably foreseeable.

194. The damages Plaintiffs and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

195. Plaintiffs and the Class have suffered injury, including as described in Section IV.B, *supra*, and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE* – *N.Y. LABOR LAW*
(On Behalf of all Plaintiffs and the Employee Subclass)

196. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

197. As a New York company, Defendant had a duty under New York Labor Law § 203-D to protect its employees' PII, including Social Security numbers, from public posting or displaying, storing it in files with unrestricted access, or communicating it to the general public.

198. Defendant violated these duties in its actions and inactions that resulted in the Data Breach.

199. The harm that has occurred is the type of harm the NY Labor Law was intended to guard against.

200. Plaintiffs and the Class Members who are or were employees of Defendant are within the class of persons who the NY Labor Law was intended to protect.

201. Defendant's breach of these duties was knowing, because it had not put in place "any policies or procedures to safeguard against such violation, including procedures to notify relevant employees of these provisions." N.Y. Labor Law § 203-D(3).

202. Plaintiffs and the Class have suffered damages as a result of Defendant's breaches of its duties, and the damages were foreseeable.

203. Defendant's violations of these duties are the proximate cause of Plaintiffs' and the Class Members' damages.

204. Plaintiffs and the Class are entitled to actual and punitive damages for Defendant's negligence *per se* in an amount to be proven at trial.

THIRD CAUSE OF ACTION
NEGLIGENCE *PER SE* – *CABLE ACT*
(On Behalf of the Plaintiffs McFarlane, Hellyer, Mason-Draffen, Raja, Gill, Frontera, Mehfooz, Paniccia and the Subscriber Subclass)

205. Plaintiffs McFarlane, Hellyer, Mason-Draffen, Raja, Gill, Frontera, Mehfooz, and Paniccia (for purposes of this Cause of Action "Plaintiffs") incorporate by reference all preceding factual allegations as though fully alleged here.

206. As a cable operator, Defendant had a duty under the Cable Communications Act of 1984, 47 U.S.C. § 551 to "not disclose" its subscribers' PII, including Social Security numbers, without prior written permission and to "take such actions as are necessary to prevent unauthorized access to such information." 47 U.S.C. § 551(c)(1).

207. Plaintiffs and the Subscriber Subclass (including current and former employees) are or were subscribers of Defendant's cable television products.

208. Defendant violated its duties under the Cable Act by its actions and inactions that caused the Data Breach.

209. The PII contained in the unencrypted report constituted "personally identifiable information" as used in the Cable Act for Plaintiffs and the Subscriber Subclass.

210. The harm that has occurred is the type of harm the Cable Act was intended to guard against.

211. Plaintiffs and the Subscriber Subclass are within the class of persons who the Cable Act was intended to protect.

212. Plaintiffs and the Subscriber Subclass have suffered damages as a result of Defendant's breaches of its duties, and the damages were foreseeable.

213. Defendant's violations of these duties are the proximate cause of Plaintiffs' and the Class Members' damages.

214. Plaintiffs and the Subscriber Subclass are entitled to actual and punitive damages for Defendant's negligence *per se* in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
NEW YORK LABOR LAW § 203-D
(On Behalf of all Plaintiffs and the Employee Subclass)

215. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

216. Under New York law, "[a]n employer shall not unless otherwise required by law: . . . (a) Publicly post or display an employee's social security number; . . . (c) Place a social security number in files with unrestricted access; or (d) Communicate an employee's personal identifying information to the general public." N.Y. Labor Law § 203-d(1).

217. "[P]ersonal identifying information" is defined as including an individual's "social security number, home address or telephone number, personal electronic mail address, Internet identification name or password, parent's surname prior to marriage, or drivers' license number." *Id.* § 203-d(1)(d).

218. The statute further provides that "[i]t shall be presumptive evidence that a violation of this section was knowing if the employer has not put in place any policies or procedures to safeguard against such violation, including procedures to notify relevant employees of these provisions." *Id.* § 203-d(3).

219. Defendant's acts and omissions were unlawful and in violation of N.Y. Labor Law § 203-d because Defendant sent an unencrypted report containing the PII of tens of thousands of Employees, including Social Security numbers, on its company email accounts, and stored it on the same unencrypted email inboxes.

220. The report containing the employee PII was unencrypted and not adequately password protected, as evidenced by the hackers' prompt circumvention of the password that was on the report.

221. Defendant, moreover, did not put into place any policies or procedures—despite its covenants stating otherwise—to safeguard against such violations, as is made evident by (i) Defendant's susceptibility to a phishing attack (of which it should have been aware by way of even minimal data security training), (ii) the fact that the files containing all of its current and former employee's PII were emailed in unencrypted format, and (iii) the fact that, rather than destroying its former employees' PII once it was no longer necessary, Altice continued to store former employees' PII in its files.

222. Accordingly, Plaintiffs and the Employee Subclass are entitled to statutory damages, compensatory damages, injunctive relief, and reasonable attorney fees and costs for Altice's violations of N.Y. Labor Law § 203-d(3).

FIFTH CAUSE OF ACTION
CABLE COMMUNICATIONS ACT OF 1984
(On Behalf of Plaintiffs McFarlane, Hellyer, Mason-Draffen, Raja, Gill, Frontera, Mehfooz, and Paniccia and the Subscriber Subclass)

223. Plaintiffs McFarlane, Hellyer, Mason-Draffen, Raja, Gill, Frontera, Mehfooz, and Paniccia (for purposes of this Cause of Action, "Plaintiffs") incorporate by reference all preceding factual allegations as though fully alleged here.

224. As Defendant acknowledges, it is a "cable provider" as defined in the Cable Communications Act of 1984 (Cable Act), 47 U.S.C. § 551.

225. Plaintiffs and members of the Subscriber Subclass are or were cable subscribers with Defendant's cable television service, including through Altice's employee cable programs, and as subscribers both before and after their employment with Altice.

226. The Cable Act provides that "a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned ***and shall take such actions as are necessary to prevent unauthorized access*** to such information by a person other than the subscriber or cable operator." 47 U.S.C. § 551(c)(1) (emphasis added).

227. Defendant violated this provision by failing to take the necessary precautions to prevent the Data Breach.

228. As a result of Defendant's violation of § 551(c)(1), Plaintiffs and the Class Members who are or were cable subscribers have suffered damages, including actual identity theft and a significantly increased risk of future harm.

229. The Cable Act also provides that "[a] cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected . . . ." *Id.* § 551(e).

230. Defendant violated this provision by failing to destroy the PII of the Subscriber Subclass members who formerly subscribed to Defendant's cable television service but have since cancelled their subscriptions, including Plaintiff Gill, who canceled her Optimum TV subscription in 2011.

231. The Cable Act provides that "[a]ny person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court." *Id.* § 551(f)(1).

232. Plaintiffs and the Subscriber Subclass were aggrieved by Defendant's violations of the Cable Act and have suffered damages. They are therefore entitled to "actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher; punitive damages; and reasonable attorneys' fees and other litigation costs reasonably incurred." *Id.* § 551(f)(2).

233. These remedies are cumulative to all other lawful remedies. *Id.* § 551(f)(3).

SIXTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of All Plaintiffs and the National Class)

234. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

235. Plaintiffs and Class Members were required to provide Defendant with their PII, including their Social Security numbers.

236. When Plaintiffs and Class Members provided their PII to Defendant when seeking employment or services, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect their PII and to timely notify them in the event of a Data Breach.

237. Based on Defendant's representations, legal obligations, and acceptance of Plaintiffs' and the Class Members' PII, Defendant had an implied duty to safeguard their PII through the use of reasonable industry standards.

238. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Altice approximately three months to warn Plaintiffs and Class Member of their imminent risk of identity theft. Defendant also failed to notify Plaintiffs and the Class Members whether or not their driver's license numbers were compromised, leaving Plaintiffs and Class Members unsure as to the extent of the information that was compromised.

239. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiffs' and the Class Members' PII.

SEVENTH CAUSE OF ACTION
INJUNCTIVE AND DECLARATORY RELIEF
(On Behalf of all Plaintiffs and the National Class)

240. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

241. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

242. As previously alleged and pleaded, Defendant owes duties of care to Plaintiffs and Class Members that requires it to adequately secure their PII.

243. Defendant still possesses the PII of Plaintiffs and the Class Members.

244. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class Members.

245. Defendant has claimed that it is taking some steps to increase its data security, but there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Breach, and to once again place profits above protection.

246. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendant to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
b. Ordering Defendant to significantly increase its spending on cybersecurity including systems and personnel;
c. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;
d. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;
e. Ordering that Defendant's segment Plaintiffs' and the Class's PII by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;
f. Ordering that Defendant cease transmitting PII via unencrypted email;
g. Ordering that Defendant cease storing PII in email accounts;

h. Ordering that Defendant conduct regular database scanning and securing checks;

i. Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

j. Ordering Defendant to implement and enforce adequate retention policies for PII, including destroying, in a reasonably secure manner, PII once it is no longer necessary for the it to be retained; and

k. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Amended Consolidated Class Action Complaint.

Dated: July 27, 2020

Respectfully submitted,

/s/ *William B. Federman*

William B. Federman
(S.D. New York #WF9124)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
wbf@federmanlaw.com

Interim Lead Class Counsel

Richard A. Acocelli
1500 Broadway, 16th Floor
New York, New York 10036
Tel: (212) 682-3025
Fax: (212) 682-3010
racocelli@weisslawllp.com

Cornelius P. Dukelow
ABINGTON COLE + ELLERY
320 South Boston Avenue, Suite 1130
Tulsa, Oklahoma 74103
Telephone and Facsimile: (918) 588-3400
cdukelow@abingtonlaw.com

Additional Plaintiffs' Counsel

CERTIFICATE OF SERVICE

I hereby certify that on July 27, 2020, a true and correct copy of the foregoing was electronically filed with the Clerk of Court using CM/ECF. Copies of the foregoing document will be served upon interested counsel via transmission of Notices of Electronic Filing generated by CM/ECF.

/s/ *William B. Federman*
William B. Federman